



日本国特許庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

CF01500205  
RECEIVED  
APR 19 2001  
Technology Center 2600

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日  
Date of Application:

1999年12月27日

出願番号  
Application Number:

平成11年特許願第371780号

願人  
Applicant(s):

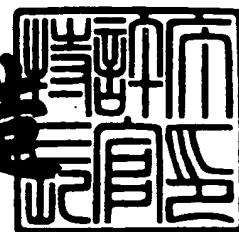
キヤノン株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年 1月19日

特許庁長官  
Commissioner,  
Patent Office

及川耕造



【書類名】 特許願

【整理番号】 4120042

【提出日】 平成11年12月27日

【あて先】 特許庁長官殿

【国際特許分類】 H04N 5/00

【発明の名称】 画像処理システム、画像処理方法、メモリカード及び記憶媒体

【請求項の数】 22

【発明者】

    【住所又は居所】 東京都大田区下丸子3丁目30番2号 キヤノン株式会社  
社内

    【氏名】 笠井 一宏

【特許出願人】

    【識別番号】 000001007

    【氏名又は名称】 キヤノン株式会社

【代理人】

    【識別番号】 100090273

    【弁理士】

    【氏名又は名称】 國分 孝悦

    【電話番号】 03-3590-8901

【手数料の表示】

    【予納台帳番号】 035493

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

    【包括委任状番号】 9705348

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 画像処理システム、画像処理方法、メモリカード及び記憶媒体

【特許請求の範囲】

【請求項 1】 メモリ媒体にアクセス可能なインターフェースを備えた画像処理システムであって、

上記メモリ媒体に蓄積されている画像ファイルデータに関する電子署名、上記電子署名に用いた秘密鍵、または上記秘密鍵と対となる公開鍵を、上記画像ファイルデータ及びプロパティファイルとともに読み出す情報読み出し手段と、

上記情報読み出し手段によって読み出された情報に基づいて画像の出力を行う画像出力制御手段とを具備することを特徴とする画像処理システム。

【請求項 2】 上記情報読み出し手段によって読み出された上記画像ファイルデータに関する電子署名を、上記公開鍵を用いて復号化する電子署名復号化手段を具備することを特徴とする請求項 1 に記載の画像処理システム。

【請求項 3】 上記画像ファイルデータから得られる画像ファイル固有のメッセージダイジェスト値を、一方向性関数を用いて算出するメッセージダイジェスト値算出手段を具備することを特徴とする請求項 1 または 2 に記載の画像処理システム。

【請求項 4】 上記画像ファイルデータの電子署名を復号化する電子署名復号化手段と、

上記電子署名復号化手段によって得られるデータ値と上記メッセージダイジェスト値とを比較する比較手段と、

上記比較手段の比較結果に基づいて、上記画像ファイルデータの検証を行う画像ファイルデータ検証手段とを具備することを特徴とする請求項 3 に記載の画像処理システム。

【請求項 5】 メモリ媒体にアクセス可能なインターフェースを備えた画像処理システムであって、

上記インターフェースに対する上記メモリ媒体の接続を検出するメモリ媒体検出手段と、

上記メモリ媒体検出手段により上記メモリ媒体の接続が検出された場合に、上

記メモリ媒体に蓄積されている画像ファイルデータに関する電子署名、上記電子署名に用いた秘密鍵、またはその対となる公開鍵を、上記画像ファイルデータ及びプロパティファイルとともに転送する情報読み出し手段と、

上記情報読み出し手段によって読み出された情報に基づいて画像出力を行うように制御する画像出力制御手段とを具備することを特徴とする画像処理システム。

【請求項6】 メモリ媒体にアクセス可能なインターフェースを備えた画像処理システムであって、

上記メモリ媒体に保存する画像ファイルデータを作成する画像ファイルデータ作成手段と、

上記画像ファイルデータ作成手段によって作成された画像ファイルデータを記憶手段に保存する画像ファイルデータ保存手段と、

上記画像ファイルデータから得られる画像ファイル固有のメッセージダイジェスト値を、一方向性関数を用いて算出するメッセージダイジェスト値算出手段と、

上記メッセージダイジェスト値算出手段により算出されたメッセージダイジェスト値を、上記記憶手段内に格納された秘密鍵で暗号化するデジタル署名生成手段とを具備することを特徴とする画像処理システム。

【請求項7】 上記デジタル署名生成手段によって作成されたデジタル署名をプロパティファイルに格納するデジタル署名格納手段と、

上記デジタル署名が格納されたプロパティファイルを上記メモリ媒体内のプロパティ領域に保存する第1の保存手段と、

上記メモリ媒体内の画像ファイル領域に署名対象画像ファイルデータを保存する第2の保存手段とを具備することを特徴とする請求項6に記載の画像処理システム。

【請求項8】 上記メッセージダイジェスト値を暗号化するための秘密鍵は機器固有の秘密鍵であることを特徴とする請求項1～7の何れか1項に記載の画像処理システム。

【請求項9】 上記メッセージダイジェスト値を暗号化するための秘密鍵をユーザ定義により新規に作成する秘密鍵作成手段を具備することを特徴とする請

求項 1～7 の何れか 1 項に記載の画像処理システム。

【請求項 10】 メモリ媒体にアクセス可能なインターフェースを備えた画像処理システムにおける画像処理方法であって、

上記メモリ媒体に蓄積されている画像ファイルデータに関する電子署名、上記電子署名に用いた秘密鍵、または上記秘密鍵と対となる公開鍵を、上記画像ファイルデータ及びプロパティファイルとともに読み出す情報読み出し処理と、

上記情報読み出し処理によって読み出された情報に基づいて画像の出力を行う画像出力制御処理とを行うことを特徴とする画像処理方法。

【請求項 11】 上記情報読み出し処理によって読み出された上記画像ファイルデータに関する電子署名を、記憶手段に格納された公開鍵を用いて復号化する電子署名復号化処理を行うことを特徴とする請求項 10 に記載の画像処理方法。

【請求項 12】 上記画像ファイルデータから得られる画像ファイル固有のメッセージダイジェスト値を、一方向性関数を用いて算出するメッセージダイジェスト値算出処理を行うことを特徴とする請求項 10 または 11 に記載の画像処理方法。

【請求項 13】 上記画像ファイルデータの電子署名を復号化する電子署名復号化処理と、

上記電子署名復号化処理によって得られるデータ値と上記メッセージダイジェスト値とを比較する比較処理と、

上記比較処理の比較結果に基づいて、上記画像ファイルデータの検証を行う画像ファイルデータ検証処理とを行うことを特徴とする請求項 12 に記載の画像処理方法。

【請求項 14】 メモリ媒体にアクセス可能なインターフェースを備えた画像処理システムにおける画像処理方法であって、

上記インターフェースに対する上記メモリ媒体の接続を検出するメモリ媒体検出処理と、

上記メモリ媒体検出処理により上記メモリ媒体の接続が検出された場合に、上記メモリ媒体に蓄積されている画像ファイルデータに関する電子署名、上記電子

署名に用いた秘密鍵、またはその対となる公開鍵を、上記画像ファイルデータ及びプロパティファイルとともに転送する情報読み出し処理と、

上記情報読み出し処理によって読み出された情報に基づいて画像出力を行うように制御する画像出力制御処理とを行うことを特徴とする画像処理方法。

【請求項 15】 メモリ媒体にアクセス可能なインターフェースを備えた画像処理システムにおける画像処理方法であって、

上記メモリ媒体に保存する画像ファイルデータを作成する画像ファイルデータ作成処理と、

上記画像ファイルデータ作成処理によって作成された画像ファイルデータを記憶手段に保存する画像ファイルデータ保存処理と、

上記画像ファイルデータから得られる画像ファイル固有のメッセージダイジェスト値を、一方向性関数を用いて算出するメッセージダイジェスト値算出処理と、

上記メッセージダイジェスト値算出処理により算出されたメッセージダイジェスト値を、上記記憶手段内に格納された秘密鍵で暗号化するデジタル署名生成処理とを行うことを特徴とする画像処理方法。

【請求項 16】 上記デジタル署名生成処理によって作成されたデジタル署名をプロパティファイルに格納するデジタル署名格納処理と、

上記デジタル署名が格納されたプロパティファイルを上記メモリ媒体内のプロパティ領域に保存する第 1 の保存処理と、

上記メモリ媒体内の画像ファイル領域に署名対象画像ファイルデータを保存する第 2 の保存処理とを行うことを特徴とする請求項 15 に記載の画像処理方法。

【請求項 17】 上記メッセージダイジェスト値を暗号化するための秘密鍵は機器固有の秘密鍵であることを特徴とする請求項 10～16 の何れか 1 項に記載の画像処理方法。

【請求項 18】 上記メッセージダイジェスト値を暗号化するための秘密鍵をユーザ定義により新規に作成する秘密鍵作成処理を行うことを特徴とする請求項 10～16 の何れか 1 項に記載の画像処理方法。

【請求項 19】 電子署名が施された画像ファイルデータが格納されている

ことを特徴とするメモリカード。

【請求項 2 0】 画像ファイルデータと、上記画像ファイルデータに関する電子署名と、上記電子署名に用いた秘密鍵と、上記秘密鍵と対となる公開鍵と、上記画像ファイルに係わるプロパティファイルとが格納されていることを特徴とするメモリカード。

【請求項 2 1】 上記請求項 1 ～ 9 の何れか 1 項に記載の各手段を構成するプログラムをコンピュータが読み出し可能に格納したことを特徴とする記憶媒体。

【請求項 2 2】 上記請求項 1 0 ～ 1 8 の何れか 1 項に記載の画像処理方法を実行するプログラムをコンピュータが読み出し可能に格納したことを特徴とする記憶媒体。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は画像処理システム、画像処理方法、メモリカード及び記憶媒体に関し、さらに詳しくは、電子署名を施すことで画像ファイルデータの信頼性を向上させることが可能な画像処理システム及び画像処理方法に関する。

【 0 0 0 2 】

【従来の技術】

従来、パーソナルコンピュータ（以下、PCと省略）、電子手帳、デジタルカメラ等で作成したデータをメモリ媒体に転送して保存した後、そのメモリ媒体を画像制御装置に接続することにより、容易に印刷を実行できるようにした画像処理システム及び画像処理方法が実用化されている。

【 0 0 0 3 】

このデータには、出力したい画像ファイルデータの他に、どの画像をどのような出力スペックで出力を行うかを記述したプロパティファイルが含まれている。

【 0 0 0 4 】

図 6 は、特開平 1 0 - 2 2 6 1 1 7 号公報で開示された画像処理システムに関するものである。この画像処理システムは、画像入出力部本体 6 1 と、画像入出

力制御装置 6 2 と、画像入出力指令キー 6 3 と、メモリカード I/F 部 6 4 と、メモリカード 6 5 とを備えている。

【0 0 0 5】

上記画像入出力制御装置 6 2 は、メモリカード 6 5 に記憶されている画像ファイルデータのうち、どのデータを画像入出力部本体 6 1 に転送してどのような出力スベツクで画像出力を行うかを記述したプロパティファイル及び該当画像ファイルデータをメモリカード 6 5 から読み出して画像出力を実行するように成されている。

【0 0 0 6】

【発明が解決しようとする課題】

しかしながら、従来のこのような画像出力方法では、メモリカードに保存された画像ファイルデータが改ざん・偽造されても、それが元来のデータなのか、それとも改ざん・偽造されたデータのなのかを区別・検証することができないという問題があった。

【0 0 0 7】

また、メモリカードが第三者の手に渡った場合、それらのデータを勝手に利用することが可能であるという問題もあった。つまり、メモリカード内のデータのセキュリティー性が欠如しており、データの信頼性を保証できない問題があった。

【0 0 0 8】

本発明は上述の問題点にかんがみ、メモリ媒体内の画像ファイルデータの改ざん・偽造を判別できるようにして、メモリ媒体からの画像出力の信頼性を向上させることを目的とする。

【0 0 0 9】

【課題を解決するための手段】

上記目的を達成するために、本発明の画像処理システムは、メモリ媒体にアクセス可能なインターフェースを備えた画像処理システムであって、上記メモリ媒体に蓄積されている画像ファイルデータに関する電子署名、上記電子署名に用いた秘密鍵、または上記秘密鍵と対となる公開鍵を、上記画像ファイルデータ及び



プロパティファイルとともに読み出して記憶手段に格納する情報読み出し手段と、上記情報読み出し手段によって読み出された情報に基づいて画像の出力を行う画像出力制御手段とを具備することを特徴としている。

また、本発明の画像処理システムの他の特徴とするところは、上記情報読み出し手段によって読み出された上記画像ファイルデータに関する電子署名を、上記記憶手段に格納された公開鍵を用いて復号化する電子署名復号化手段を具備することを特徴としている。

また、本発明の画像処理システムのその他の特徴とするところは、上記画像ファイルデータから得られる画像ファイル固有のメッセージダイジェスト値を、一方向性関数を用いて算出するメッセージダイジェスト値算出手段を具備することを特徴としている。

また、本発明の画像処理システムのその他の特徴とするところは、上記画像ファイルデータの電子署名を復号化する電子署名復号化手段と、上記電子署名復号化手段によって得られるデータ値と上記メッセージダイジェスト値とを比較する比較手段と、上記比較手段の比較結果に基づいて、上記画像ファイルデータの検証を行う画像ファイルデータ検証手段とを具備することを特徴としている。

また、本発明の画像処理システムのその他の特徴とするところは、メモリ媒体にアクセス可能なインターフェースを備えた画像処理システムであって、上記インターフェースに対する上記メモリ媒体の接続を検出するメモリ媒体検出手段と、上記メモリ媒体検出手段により上記メモリ媒体の接続が検出された場合に、上記メモリ媒体に蓄積されている画像ファイルデータに関する電子署名、上記電子署名に用いた秘密鍵、またはその対となる公開鍵を、上記画像ファイルデータ及びプロパティファイルとともに転送する情報読み出し手段と、上記情報読み出し手段によって読み出された情報に基づいて画像出力を行うように制御する画像出力制御手段とを具備することを特徴としている。

また、本発明の画像処理システムのその他の特徴とするところは、メモリ媒体にアクセス可能なインターフェースを備えた画像処理システムであって、上記メモリ媒体に保存する画像ファイルデータを作成する画像ファイルデータ作成手段と、上記画像ファイルデータ作成手段によって作成された画像ファイルデータを

記憶手段に保存する画像ファイルデータ保存手段と、上記画像ファイルデータから得られる画像ファイル固有のメッセージダイジェスト値を、一方向性関数を用いて算出するメッセージダイジェスト値算出手段と、

上記メッセージダイジェスト値算出手段により算出されたメッセージダイジェスト値を、上記記憶手段内に格納された秘密鍵で暗号化するデジタル署名生成手段とを具備することを特徴としている。

また、本発明の画像処理システムのその他の特徴とするところは、上記デジタル署名生成手段によって作成されたデジタル署名をプロパティファイルに格納するデジタル署名格納手段と、上記デジタル署名が格納されたプロパティファイルを上記メモリ媒体内のプロパティ領域に保存する第 1 の保存手段と、上記メモリ媒体内の画像ファイル領域に署名対象画像ファイルデータを保存する第 2 の保存手段とを具備することを特徴としている。

また、本発明の画像処理システムのその他の特徴とするところは、上記メッセージダイジェスト値を暗号化するための秘密鍵は機器固有の秘密鍵であることを特徴としている。

また、本発明の画像処理システムのその他の特徴とするところは、上記メッセージダイジェスト値を暗号化するための秘密鍵をユーザ定義により新規に作成する秘密鍵作成手段を具備することを特徴としている。

#### 【 0 0 1 0 】

本発明の画像処理方法は、メモリ媒体にアクセス可能なインターフェースを備えた画像処理システムにおける画像処理方法であって、上記メモリ媒体に蓄積されている画像ファイルデータに関する電子署名、上記電子署名に用いた秘密鍵、または上記秘密鍵と対となる公開鍵を、上記画像ファイルデータ及びプロパティファイルとともに読み出して記憶手段に格納する情報読み出し処理と、上記情報読み出し処理によって読み出された情報に基づいて画像の出力を行う画像出力制御処理とを行うことを特徴としている。

また、本発明の画像処理方法の他の特徴とするところは、上記情報読み出し処理によって読み出された上記画像ファイルデータに関する電子署名を、上記記憶手段に格納された公開鍵を用いて復号化する電子署名復号化処理を行うことを特

徴としている。

また、本発明の画像処理方法のその他の特徴とするところは、上記画像ファイルデータから得られる画像ファイル固有のメッセージダイジェスト値を、一方向性関数を用いて算出するメッセージダイジェスト値算出処理を行うことを特徴としている。

また、本発明の画像処理方法のその他の特徴とするところは、上記画像ファイルデータの電子署名を復号化する電子署名復号化処理と、上記電子署名復号化処理によって得られるデータ値と上記メッセージダイジェスト値とを比較する比較処理と、上記比較処理の比較結果に基づいて、上記画像ファイルデータの検証を行う画像ファイルデータ検証処理とを行うことを特徴としている。

また、本発明の画像処理方法のその他の特徴とするところは、メモリ媒体にアクセス可能なインターフェースを備えた画像処理システムにおける画像処理方法であって、上記インターフェースに対する上記メモリ媒体の接続を検出するメモリ媒体検出処理と、上記メモリ媒体検出処理により上記メモリ媒体の接続が検出された場合に、上記メモリ媒体に蓄積されている画像ファイルデータに関する電子署名、上記電子署名に用いた秘密鍵、またはその対となる公開鍵を、上記画像ファイルデータ及びプロパティファイルとともに転送する情報読み出し処理と、上記情報読み出し処理によって読み出された情報に基づいて画像出力を行うように制御する画像出力制御処理とを行うことを特徴としている。

また、本発明の画像処理方法のその他の特徴とするところは、メモリ媒体にアクセス可能なインターフェースを備えた画像処理システムにおける画像処理方法であって、上記メモリ媒体に保存する画像ファイルデータを作成する画像ファイルデータ作成処理と、上記画像ファイルデータ作成処理によって作成された画像ファイルデータを記憶手段に保存する画像ファイルデータ保存処理と、上記画像ファイルデータから得られる画像ファイル固有のメッセージダイジェスト値を、一方向性関数を用いて算出するメッセージダイジェスト値算出処理と、上記メッセージダイジェスト値算出処理により算出されたメッセージダイジェスト値を、上記記憶手段内に格納された秘密鍵で暗号化するデジタル署名生成処理とを行うことを特徴としている。

また、本発明の画像処理方法のその他の特徴とするところは、上記デジタル署名生成処理によって作成されたデジタル署名をプロパティファイルに格納するデジタル署名格納処理と、上記デジタル署名が格納されたプロパティファイルを上記メモリ媒体内のプロパティ領域に保存する第 1 の保存処理と、上記メモリ媒体内の画像ファイル領域に署名対象画像ファイルデータを保存する第 2 の保存処理とを行うことを特徴としている。

また、本発明の画像処理方法のその他の特徴とするところは、上記メッセージダイジェスト値を暗号化するための秘密鍵は機器固有の秘密鍵であることを特徴としている。

また、本発明の画像処理方法のその他の特徴とするところは、上記メッセージダイジェスト値を暗号化するための秘密鍵をユーザ定義により新規に作成する秘密鍵作成処理を行うことを特徴としている。

#### 【 0 0 1 1 】

本発明のメモリカードは、電子署名が施された画像ファイルデータが格納されていることを特徴としている。

また、本発明のメモリカードの他の特徴とするところは、画像ファイルデータと、上記画像ファイルデータに関する電子署名と、上記電子署名に用いた秘密鍵と、上記秘密鍵と対となる公開鍵と、上記画像ファイルに係わるプロパティファイルとが格納されていることを特徴としている。

#### 【 0 0 1 2 】

本発明の記憶媒体は、上記記載の各手段を構成するプログラムをコンピュータから読み出し可能に格納したことを特徴としている。

また、本発明の記憶媒体の他の特徴とするところは、上記画像処理方法を実行するプログラムをコンピュータから読み出し可能に格納したことを特徴としている。

#### 【 0 0 1 3 】

#### 【発明の実施の形態】

次に、本発明画像処理システム、画像処理方法、メモリカード及び記憶媒体の実施の形態を、図面を参照しながら説明する。

(第 1 の実施の形態)

図 1 は、第 1 の実施形態における画像処理システムの全体構成を示すブロック図である。図 1 に示したように、この画像処理システムはリーダ部（画像入力装置）200と、プリンタ部（画像出力装置）300とで構成されている。

【0014】

リーダ部（画像入力装置）200は、原稿画像を光学的に読み取り、画像データに変換するものであり、原稿を読み取るための機能を持つスキャナユニット210と、原稿用紙を搬送するための機能を持つ原稿給紙ユニット250とで構成されている。

【0015】

また、プリンタ部（画像出力装置）300は、記録紙を搬送し、その上に画像データを可視画像として印字して装置外に排紙するものであり、複数種類の記録紙カセットを持つ給紙ユニット310と、画像データを記録紙に転写、定着させる機能を持つマーキングユニット320と、印字された記録紙をソート、ステイプルして機外へ出力する機能を持つ排紙ユニット330とで構成されている。

【0016】

また、本実施形態の画像処理システム100は、メモリカードインターフェース（I/F）部270と、制御装置110とを具備しており、メモリカードインターフェース（I/F）部270は、メモリカード275に蓄積されているデータを読み取ったり、制御装置110の記憶手段111に蓄積されているデータをメモリカード275に書き込んだりする。

【0017】

また、制御装置110は、リーダ部200、プリンタ部300、メモリカード（I/F）部270と電氣的に接続され、さらにネットワーク400を介して、ホストコンピュータ401、402と接続されている。

【0018】

さらに、上記制御装置110は、CPU、ROM、RAM等からなるコンピュータシステムにより構成されており、本実施形態の情報読み出し手段、画像出力制御手段、電子署名復号化手段、メッセージダイジェスト値算出手段、電子署名

復号化手段、比較手段、画像ファイルデータ検証手段、メモリ媒体検出手段、画像ファイルデータ作成手段、画像ファイルデータ保存手段、デジタル署名生成手段、デジタル署名格納手段、第 1 の保存手段、第 2 の保存手段及び秘密鍵作成手段等が上記コンピュータシステムのプログラムによって構成されている。

【 0 0 1 9 】

上述のような各手段を構成する制御装置 1 1 0 は、リーダ部 2 0 0 を制御して、原稿の画像データを読み込み、プリンタ部 3 0 0 を制御して画像データを記録用紙に出力してコピー機能を提供する。

【 0 0 2 0 】

また、リーダ部 2 0 0 やメモリカード (I/F) 部 2 7 0 から読み取った画像データをコードデータに変換し、ネットワーク 4 0 0 を介してホストコンピュータへ送信するスキャナ機能、ホストコンピュータからネットワーク 4 0 0 を介して受信したコードデータを画像データに変換し、プリンタ部 3 0 0 に出力するプリンタ機能を提供する。

【 0 0 2 1 】

操作部 1 5 0 は、制御装置 1 1 0 に接続され、液晶タッチパネルで構成され、画像処理システムを操作するためのユーザ (I/F) を提供する。

【 0 0 2 2 】

図 2 は、リーダ部 2 0 0 及びプリンタ部 3 0 0 の概略構成を示す断面図である。リーダ部 2 0 0 の原稿給送ユニット 2 5 0 は、原稿を先頭順に 1 枚ずつプラテンガラス 2 1 1 上へ給送し、原稿の読み取り動作終了後、プラテンガラス 2 1 1 上の原稿を排出するものである。

【 0 0 2 3 】

上記制御装置 1 1 0 は、原稿がプラテンガラス 2 1 1 上に搬送されると、ランプ 2 1 2 を点灯する。また、光学ユニット 2 1 3 の移動を開始させて、原稿を露光走査する。この時の原稿からの反射光は、ミラー 2 1 4, 2 1 5, 2 1 6、及びレンズ 2 1 7 によって CCD イメージセンサ (以下、CCD という) 2 1 8 へ導かれる。

【 0 0 2 4 】

このように、走査された原稿の画像はCCD 2 1 8によって読み取られる。CCD 2 1 8から出力される画像データは、所定の処理が施された後、制御装置 1 1 0へ転送される。

【0 0 2 5】

プリンタ部 3 0 0のレーザドライバ 3 2 1は、レーザ発光部 3 2 2を駆動するものであり、制御装置 1 1 0から出力された画像データに応じたレーザ光をレーザ発光部 3 2 2により発光させる。

【0 0 2 6】

このレーザ光は、感光ドラム 3 2 3に照射され、感光ドラム 3 2 3にはレーザ光に応じた潜像が形成される。この感光ドラム 3 2 3の潜像の部分には現像器 3 2 4によって現像剤が付着される。

【0 0 2 7】

そして、レーザ光の照射開始と同期したタイミングで、カセット 3 1 1及びカセット 3 1 2のいずれかから記録紙を給紙して転写部 3 2 5へ搬送し、感光ドラム 3 2 3に付着された現像剤を記録紙に転写する。現像剤の乗った記録紙は定着部 3 2 6に搬送され、この定着部 3 2 6の熱と圧力により現像剤は記録紙に定着される。

【0 0 2 8】

定着部 3 2 6を通過した記録紙は、次に排出口ローラ 3 2 7によって排出される。排紙ユニット 3 3 0は、排出された記録紙を束ねて記録紙の仕分けをしたり、仕分けされた記録紙のステイプルを行う。

【0 0 2 9】

また、両面記録が設定されている場合は、排出口ローラ 3 2 7のところまで記録紙を搬送した後、排出口ローラ 3 2 7の回転方向を逆転させ、フラップ 3 2 8によって再給紙搬送路 3 2 9へ導く。再給紙搬送路 3 2 9へ導かれた記録紙は上述したタイミングで転写部 3 2 5へ給紙される。

【0 0 3 0】

上述のように構成された画像処理システムにおいて、本実施形態ではメモリカード内の画像ファイルデータに電子署名を施すことで、メモリカード内の画像フ

ファイルデータの信頼性を向上させるようにしている。この電子署名技術として現在、R S A (Rivest#Shamir#Adelman) 方式などの、いわゆる非対称公開鍵方式を利用したものが知られている。上記非対称公開鍵方式は、「公開鍵」と「秘密鍵」という一対の鍵情報を設定している。

#### 【0031】

図3及び図4は、上記電子署名について概念的に説明したものである。この技術においては、図4中の「メッセージダイジェスト値」と「公開鍵」がポイントとなっている。上記メッセージダイジェスト値は、個々のメッセージに対し固有の値を持っている。

#### 【0032】

まず、署名したいデータ（テキストやバイナリ）に対して、メッセージダイジェスト値を算出する。上記メッセージダイジェスト値は、一方向性関数（ハッシュ関数）を用いて、署名したいデータから作成されるものであり、データに固有の値である。そして、上記のように作成されたメッセージダイジェスト値を秘密鍵で暗号化する。

#### 【0033】

電子的データの送受信を行う場合、送信側は上記秘密鍵で暗号化されたメッセージダイジェスト値を署名として、署名対象データとともに受信側に送り出す。受信側は、受信した署名データを署名側の公開鍵で復号化してメッセージダイジェスト値を得る。

#### 【0034】

そして、受信した署名対象データから算出されるメッセージダイジェスト値と、上記復号化したメッセージダイジェスト値とを比較する。上記のような手順で署名の検証を行うことにより電子署名が実現されている。

#### 【0035】

図7は、メモ리카ード275のメモリマップの一例を示す図であり、画像ファイルデータ及びプロパティファイルが保存されている。プロパティファイルは、基本的に基本的にASCIIコードのみで使用したText形式により記載されており、プリントジョブごとに指定情報が完結する記述となっている。また、プロパ



ティファイルはメモ리카ード内に1つ存在し、対象となる画像ファイルデータは保存場所を問わない。さらに、このプロパティファイルは、対象装置以外書き込み不可と設定可能なデータ記憶領域を持つ。

## 【0036】

次に、上記構成からなる第1の実施形態に係わるメモ리카ードを利用した画像ファイルデータ改ざん防止方法を備えた画像処理システムの制御手順の一例について、図1及び図2の装置構成図及び図10のフローチャートを用いて説明する。

## 【0037】

本実施形態では、図5に示すように、MD5と呼ばれるハッシュ関数を用いて署名したいデータのメッセージダイジェスト値を算出するようにしている。上記MD5は、暗号化プログラムの1つであるPGP (Pretty Good Privacy) で現在実際に使われているメッセージダイジェスト関数である。

## 【0038】

本実施形態に係わる画像処理システムでは、図7のメモリマップを有するメモ리카ード275がメモ리카ード(I/F)部270と接続された状態で制御が行われる。この時のプロパティファイルのプリントジョブ記述例は、図8のように「pic1.jpg,A4,SS,1p」となっており、それぞれ出力ファイル名=“pic1.jpg”、出力紙サイズ=“A4”、片面印刷、出力部数=1枚、という指定となっている。

メモ리카ード275内の画像ファイルデータを出力させる場合、ユーザは操作部150のメモ리카ード内画像データ出力キーを押下することにより、画像データファイルの検証・出力制御が開始される。

## 【0039】

制御装置110は、メモ리카ード(I/F)部270を介してメモ리카ード275に、画像処理システムにて出力するデータが蓄積されているかどうか確認する(ステップS1001)。例えば、メモ리카ード275内には、図7のメモリマップに示すように、2つの画像ファイルデータ(pic1.jpgとpic2.jpg)、画像ファイルデータpic1の署名(pic1.asc)、公開鍵(publickey.asc)、そしてプロパティ

ファイル (autprint.mrk) とが蓄積されており、それらのデータをメモリカード (I/F) 部 270 を介して制御装置 110 に転送する (ステップ S1002)。  
データが蓄積されてない場合は、この制御を終了する。

#### 【0040】

次に、制御装置 110 は、転送された各画像ファイルデータについて対応する画像に関する電子署名が存在するか確認する (ステップ S1003)。この例では、pic1.asc が pic1.jpg の電子署名となる。電子署名が存在しなければ、その画像ファイルデータには電子署名が施されていないと判断し、暗号検証の処理を行わずプロパティファイルに記述されたプリントジョブ情報に基づいて画像を出力する。

#### 【0041】

一方、電子署名が存在するならば、その電子署名を復号化するための公開鍵が画像処理システムに存在するか否かを確認し (ステップ S1004)、公開鍵が存在しなければ操作部に「公開鍵が滞在しない」というメッセージを表示させる。この時、ユーザは暗号検証をせずにプロパティファイルに記述されたプリントジョブ情報に基づいて画像を出力するか、この制御を終了するかのどちらかを、操作部 150 において選択・指示する。

#### 【0042】

公開鍵が存在するならば (この例であれば、publickey.asc)、それを用いて電子署名からメッセージダイジェスト値を算出する (ステップ S1005)。また、画像ファイルデータからもメッセージダイジェスト値を算出し (ステップ S1006)、この 2 つの MD 値を検証する (ステップ S1007)。

#### 【0043】

上記検証の結果が合致すれば、この画像ファイルデータは改ざんされていないと判定でき、プロパティファイルに記述されたプリントジョブ情報に基づいて画像出力処理を行う (ステップ S1009)。

#### 【0044】

また、上記判定の結果、合致しなければ、この画像ファイルデータは改ざんされたものと判定できるので、操作部に「署名不一致」というエラーメッセージを

表示させる。

【0045】

ユーザは、改ざんされた画像をプロパティファイルに記述されたプリントジョブ情報に基づいて出力するか、もしくはこの制御を終了するかを操作部150において選択・指示し（ステップS1008）、その後、この制御を終了する。

【0046】

（第2の実施の形態）

上述した第1の実施形態では、ユーザの指示によりメモ리카ード内の画像ファイルデータを出力する方法を述べたが、第2の実施形態では、メモ리카ード内のプロパティファイルに上記第1の実施形態でユーザに委ねる選択を記述し、操作部150のメモ리카ード内画像データ出力キーの押下、もしくは制御装置110によるメモ리카ード(I/F)部270へのメモ리카ード275の挿入検出により、上記選択された指示通り制御を行う方法について、図1、2の装置構成図、及び図11のフローチャートを用いて説明する。

【0047】

本実施の形態に係わる画像処理システムでは、第1の実施形態と同様に、図7のメモリマップを有するメモ리카ード275がメモ리카ード(I/F)部270と接続された状態で制御が行われる。この時のプロパティファイルのプリントジョブ記述例は、図9のように「pic1.jpg , A4, SS, 1P, NK1, UM0」となっており、それぞれ出力ファイル名＝“pic1.jpg”、出力紙サイズ＝“A4”、片面印刷、出力部数＝1枚、公開鍵が存在しない時＝出力する、署名検証不一致の時＝出力しない、という指定となっている。

【0048】

メモ리카ード275内の画像ファイルデータを出力させる場合、ユーザは操作部150のメモ리카ード内画像データ出力キーを押下、もしくは制御装置110によるメモ리카ード(I/F)部270へのメモ리카ード275の挿入検出により画像データファイルの検証・出力制御が開始される。

【0049】

制御装置110は、メモ리카ード(I/F)部270を介してメモ리카ード250

に、画像処理システムにて出力するデータが蓄積されているかどうか確認し（ステップS1101）、蓄積されていればそれらのデータをメモリカード（I/F）部270を介して制御装置110に転送する（ステップS1102）。一方、データが蓄積されてない場合は、この制御を終了する。

#### 【0050】

次に、制御装置110は、転送された各画像ファイルデータについて対応する画像に関する電子署名が存在するか確認する（ステップS1103）。この例では、pic1.Accがpic1.jpgの電子署名となる。

#### 【0051】

電子署名が存在しなければその画像ファイルデータには電子署名が施されていないと判断し、暗号検証の処理を行わずプロパティファイルに記述されたプリントジョブ情報に基づいて画像を出力する（ステップS1109）。

#### 【0052】

電子署名が存在するならば、その電子署名を復号化するための公開鍵が画像処理システムに存在するか確認し（ステップS1104）、公開鍵が存在しなければ操作部に「公開鍵が存在しない」というメッセージを表示させ、暗号検証をせずにプロパティファイルに記述されたプリントジョブ情報に基づいて画像を出力するか、この制御を終了するかを、プロパティファイルに記述された制御方法（図9の場合だと、出力する）に基づいて制御を行う。

#### 【0053】

公開鍵が存在するならば、それを用いて電子署名からメッセージダイジェスト値を算出し（ステップS1105）、また、画像ファイルデータからもメッセージダイジェスト値を算出し（ステップS1106）、この2つのMD値を検証する（ステップS1107）。

#### 【0054】

上記検証の結果、合致すれば、該画像ファイルデータは改ざんされていないと判定でき、プロパティファイルに記述されたプリントジョブ情報に基づいて画像出力処理を行う。もし、合致しなければ、該画像ファイルデータは改ざんされたものと半淀でき、操作部に「署名不一致」というエラーメッセージを表示させる

【 0 0 5 5 】

そして、改ざんされた画像をプロパティファイルに記述されたプリントジョブ情報に基づいて出力するかもしれないこの撮脚を終了するかを、プロパティファイルに記述された制御方法（図 9 の場合だと、出力しない）に基づいて制御を行い（ステップ S 1 1 0 8）、その後、この制御を終了する。

【 0 0 5 6 】

（第 3 の実施の形態）

第 1 の実施形態及び第 2 の実施形態においては、画像処理システムのメモ리카ード(I/F)を介してメモ리카ードに蓄積された画像ファイルデータの検証、出力方法に関して述べた。

【 0 0 5 7 】

この第 3 の実施形態では、画像処理システムがネットワークを介してホストコンピュータと接続されていることを利用して、ホストコンピュータのメモ리카ード(I/F)を介してメモ리카ードに蓄積されている画像ファイルデータ、画像ファイルデータの電子署名、プロパティファイルなどを画像処理システムに転送し、画像の検証・出力を行う方法について、図 1， 2 の装置構成図、及び図 1 2 のフローチャートを用いて説明する。

【 0 0 5 8 】

本実施の形態に係わる画像処理システムでは、第 1 の実施形態、第 2 の実施形態と同様に、メモ리카ード 4 0 4 がメモ리카ード(I/F) 4 0 3 と接続された状態で制御が行われる。

【 0 0 5 9 】

メモ리카ード 4 0 4 内の画像ファイルデータをホストコンピュータ 4 0 1 側で取り込み、ネットワーク 4 0 0 を介して画像処理システム 1 0 0 の制御装置 1 1 0 に転送して出力させる場合、ユーザはホストコンピュータ 4 0 1 を操作して制御を開始するか、もしくは、画像処理システム 1 0 0 の操作部 1 5 0 においてネットワーク 4 0 0 に接続されているホストコンピュータ 4 0 1 を介してメモ리카ード 4 0 4 内画像データを取り込み、出力するキーを押下することにより、画像

データファイルの取り込み・検証・出力制御が開始される。

【0060】

制御装置110は、ネットワーク接続されているホストコンピュータ401のメモリカード(I/F)403を介してメモリカード404に出力するデータが蓄積されているかどうか確認し(ステップS1201)、蓄積されていればそれらのデータをメモリカード(I/F)403及びネットワーク400を介して制御装置110に転送する(ステップS1202)。データが蓄積されてない場合は、この制御を終了する。また、該当プログラムが制御装置110に存在しない場合には、そのプログラムをネットワーク400を介してホストコンピュータ401より制御装置110に転送する。

【0061】

次に、制御装置110は転送された各画像ファイルデータについて対応する画像に関する電子署名が存するか確認する(ステップS1203)。この確認の結果、電子署名が存在しなければ、その画像ファイルデータには電子署名が施されていないと判断し、暗号検証の処理を行わずプロパティファイルに記述されたプリントジョブ情報に基づいて画像を出力する(ステップS1209)。

【0062】

一方、上記確認の結果、電子署名が存在するならば、その電子署名を復号化するための公開鍵が画像処理システムに存在するか確認(ステップS1204)し、公開鍵が存在しないならば操作部150もしくはホストコンピュータ401に「公開鍵が存在しない」というメッセージを表示させ、暗号検証をせずにプロパティファイルに記述されたプリントジョブ情報に基づいて画像を出力するかこの制御を終了するかを、操作部150またはホストコンピュータ401において選択・指示するか、もしくはプロパティファイルに記述された撮御方法(図9の場合だと、出力する)に基づいて制御を行う。

【0063】

公開鍵が存在するならば、それを用いて電子署名からメッセージダイジェスト値を算出し(ステップS1205)、また、画像ファイルデータからもメッセージダイジェスト値を算出し(ステップS1206)、この2つのMD値を検証す

る（ステップS1207）。

【0064】

合致すれば、該画像ファイルデータは改ざんされていないと判定でき、プロパティファイルに記述されたプリントジョブ情報に基づいて画像出力処理を行う（ステップS1209）。もし合致しなければ、該画像ファイルデータは改ざんされたものと判定でき、操作部150またはホストコンピュータ401に「署名不一致」というエラーメッセージを表示させる。

【0065】

そして、改ざんされた画像をプロパティファイルに記述されたプリントジョブ情報に基づいて出力するかもしれないか、この制御を終了するかを、操作部150またはホストコンピュータ401において選択・指示するか、もしくはプロパティファイルに記述された制御方法（図9の場合だと、出力しない）に基づいて制御を行い（ステップS1208）、その後、この制御を終了する。

【0066】

（第4の実施の形態）

第4の実施形態では、画像処理システムのリーダ部もしくはネットワークを介して接続されているホストコンピュータにより取り込まれた画像を制御装置内の秘密鍵を用いて署名し、画像ファイルデータ、その電子署名、及びプロパティファイルをメモリカードに保存する方法について説明する。

【0067】

ある原稿を画像処理システムのリーダ部200にて取り込み、その画像データをメモリカードに保存しようとする時、操作部150にてその制御の実行開始ボタン等を押下することにより、この制御が開始される。

【0068】

まず、原稿読み取りの制御手順に関して、図2の断面図を用いて説明する。原稿がプラテンガラス211上に搬送されると、ランプ212を点灯させる。そして、光学ユニット213の移動を開始させて、原稿を露光走査する。この時の原稿からの反射光は、ミラー214、215、216、及びレンズ217によってCCDイメージセンサ（以下CCDという）218へ導かれる。

【 0 0 6 9 】

このように、走査された原稿の画像は C C D 2 1 8 によって読み取られる。C C D 2 1 8 から出力される画像データは、所定の処理が施された後、制御装置 1 1 0 へ転送される。

【 0 0 7 0 】

一方、ホストコンピュータ 4 0 1, 4 0 2 にある画像ファイルデータをネットワーク 4 0 0 を介して制御装置 1 1 0 に転送し、その画像ファイルデータをメモ리카ード 2 7 5 に保存しようとする時は、ホストコンピュータ 4 0 1, 4 0 2 もしくは操作部 1 5 0 に配設されている制御開始ボタンを押下することによりこの制御が開始され、画像ファイルデータはネットワーク 4 0 0 を介して画像処理システムの制御装置 1 1 0 に転送される。

【 0 0 7 1 】

以後の制御は、画像ファイルデータをリーダ部 2 0 0 で読み取った場合と、ホストコンピュータ 4 0 1, 4 0 2 からネットワーク 4 0 0 を介して転送した場合と同様となり、図 1 3 のフローチャートを用いて説明する。

【 0 0 7 2 】

制御装置 1 1 0 は、取り込んだ画像をメモ리카ード 2 7 5 に保存する時、電子署名を行うかどうかユーザに確認するため、操作部 1 5 0 もしくはホストコンピュータ 4 0 1, 4 0 2 にその意向を表示して、データに電子署名を行うか否かを選択させる（ステップ S 1 3 0 1）。

【 0 0 7 3 】

図 1 5 は、この意向表示の一例であり、これに限定されるものではない。署名を行わない場合は、すぐさまメモ리카ード 2 7 5 にその画像ファイルデータを保存して（ステップ S 1 3 1 1）、制御処理を終了する。

【 0 0 7 4 】

一方、署名を行う場合、秘密鍵を新規に作成するか否かを選択させる（ステップ S 1 3 0 2）。この結果、秘密鍵を新規に作成する場合には秘密鍵暗証番号の入力を行い（ステップ S 1 3 0 2）、その後、秘密鍵の作成・保存を行う（ステップ S 1 3 0 4）。その後、公開鍵の作成・保存を行う（ステップ S 1 3 0 5）



【0075】

また、秘密鍵を新規に作成しない場合には、システムに保存された秘密鍵を選択し（ステップS1306）、公開鍵が存在するか否かを判定する（ステップS1307）。この判定の結果、存在する場合にはステップS1305に進んで公開鍵の作成・保存を行う。

【0076】

次に、署名対象ファイルデータのメッセージダイジェスト値を算出し（ステップS1308）、上記メッセージダイジェスト値を秘密鍵で暗号化し（ステップS1309）、この暗号化されたメッセージダイジェスト値を署名としてメモリカードに保存する（ステップS1310）。

【0077】

この秘密鍵や対となる公開鍵は、署名時にユーザ自身が新たに作成することもできるし、また、画像処理システムに保有されているものを用いることもできる。ユーザが秘密鍵を作成する場合、制御装置はユーザに対して任意の暗証番号を入力してもらうことにより自動的に秘密鍵、公開鍵を作成する。その後、署名対象となった画像ファイルデータをメモリカードに保存する（ステップS1311）。

【0078】

次に、プリントジョブデータの作成を行うか否かを選択させるために、制御装置は操作部150もしくはホストコンピュータ401、402にその意向を表示する（ステップS1312）。

【0079】

図16は、この意向表示の一例であり、これに限定されるものではない。プリントジョブデータの作成を行う場合、ユーザは操作部において、出力用紙サイズ、枚数、オプションなどといったプリントジョブ項目を選択し、その選択したプリントジョブデータをメモリカードのプロパティファイルに保存する（ステップS1313）。

【0080】

次に、制御装置 1 1 0 は、画像を署名する時に用いた秘密鍵やその対となる公開鍵をメモリカードに保存するかどうかユーザに確認する。図 1 7 は、この意向表示の一例であるが、これに限定されるものではない。

【 0 0 8 1 】

次に、秘密鍵、公開鍵の保存、表示方法について、図 1 4 のフローチャートを用いて説明する。

最初に、秘密鍵・公開鍵を保存、表示するか否かの選択を行わせ（ステップ S 1 4 0 0）、保存、表示を行わない場合には処理を終了する。また、処理を行う場合には、これらの鍵の保存・表示方法について選択する項目が出力装置に表示される（ステップ S 1 4 0 2）。

【 0 0 8 2 】

図 1 8 は、この意向表示の一例であり、これに限定されるものではない。特に公開鍵は、上記画像ファイルデータと上記署名との検証に用いられるため、何らかの方法で保存しておく必要がある。これらの扱いについては、以下のような選択肢がある。

【 0 0 8 3 】

公開鍵について、

- （１）公開鍵を画像ファイルデータと署名が保存されているメモリカードと同一のメモリカードに保存する。
- （２）公開鍵を画像ファイルデータと署名が保存されているメモリカードと別のメモリカードに保存する。
- （３）公開鍵を操作部に表示する。

【 0 0 8 4 】

秘密鍵について、

- （１）秘密鍵を画像ファイルデータと署名が保存されているメモリカードと同一のメモリカードに保存する。
- （２）秘密鍵を画像ファイルデータと署名が保存されているメモリカードと別のメモリカードに保存する。
- （３）秘密鍵を操作部に表示する。

【0085】

上記秘密鍵、上記公開鍵の保存・表示方法を選択した結果、保存・表示を行わない場合には処理を終了する。

一方、公開鍵の保存・表示を行う場合には、ユーザに保存・表示形態について確認させる(ステップS1402)。

【0086】

次に、署名付き画像ファイルデータを保存しているメモリカードと同一メモリカードに秘密鍵を保存するか否かを決めさせる(ステップS1403)。この判定の結果、同じメモリカードに保存しない場合にはステップS1405に進む。また、同じメモリカードに保存する場合は、画像ファイルデータが保存されているメモリカードに秘密鍵を保存する(ステップS1404)。その後、ステップS1405に進む。

【0087】

次に、ステップS1405では、秘密鍵をデータとは別のメモリカードに保存するか否かを決定させる。この結果、秘密鍵を署名付き画像ファイルデータと別のメモリカードに保存する場合、ステップS1406に進んで秘密鍵保存フラグをオンにし、その後、ステップS1407に進む。

【0088】

ステップS1407では、秘密鍵を表示するか否かを判定し、表示する場合にはステップS1408に進んで秘密鍵を表示する。また、表示しない場合にはステップS1409に進む。

【0089】

ステップS1409では、署名付き画像ファイルデータを保存しているメモリカードと同一メモリカードに公開鍵を保存するか否かを決めさせる。この判定の結果、同じメモリカードに保存しない場合にはステップS1411に進む。また、同じメモリカードに保存する場合は、画像ファイルデータが保存されているメモリカードに公開鍵を保存する(ステップS1410)。その後、ステップS1411に進む。

【0090】

次に、ステップ S 1 4 1 1 では、公開鍵をデータとは別のメモリカードに保存するか否かを決定させる。この結果、公開鍵を署名付き画像ファイルデータと別のメモリカードに保存する場合、ステップ S 1 4 1 2 に進んで公開鍵保存フラグをオンにし、その後、ステップ S 1 4 1 3 に進む。

【0 0 9 1】

ステップ S 1 4 1 3 では、公開鍵を表示するか否かを判定し、表示する場合にはステップ S 1 4 1 4 に進んで公開鍵を表示する。また、表示しない場合にはステップ S 1 4 1 5 に進む。

【0 0 9 2】

ステップ S 1 4 1 5 では、秘密鍵フラグまたは公開鍵フラグがオンになっているか否かを判定する。この判定の結果、フラグがオンになっている場合には、ステップ S 1 4 1 6 に進んでメモリカードを交換するようユーザに指示した後に、交換されたメモリカードを認識し、その後、秘密鍵をフラグがオンの鍵をメモリカードに保存する（ステップ S 1 4 1 7）。

【0 0 9 3】

これらの秘密鍵や公開鍵、そして署名や画像ファイルデータは、ユーザの選択によりメモリカード 2 7 5 の対象装置以外の書き込み不可領域に保存することもできる（ステップ S 1 4 1 1 及びステップ 1 4 1 2）。

【0 0 9 4】

（本発明の他の実施の形態）

本発明は複数の機器（例えば、ホストコンピュータ、インターフェース機器、リーダ、プリンタ等）から構成されるシステムに適用しても 1 つの機器からなる装置に適用しても良い。

【0 0 9 5】

また、上述した実施の形態の機能を実現するように各種のデバイスを動作させるように、上記各種デバイスと接続された装置あるいはシステム内のコンピュータに対し、上記実施の形態の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステムあるいは装置のコンピュータ（CPU あるいは MPU）に格納されたプログラムに従って上記各種デバイスを動作させることによっ

て実施したものの、本発明の範疇に含まれる。

【0096】

また、この場合、上記ソフトウェアのプログラムコード自体が上述した実施の形態の機能を実現することになり、そのプログラムコード自体、及びそのプログラムコードをコンピュータに供給するための手段、例えばかかるプログラムコードを格納した記憶媒体は本発明を構成する。かかるプログラムコードを記憶する記憶媒体としては、例えばフロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、磁気テープ、不揮発性のメモリカード、ROM等を用いることができる。

【0097】

また、コンピュータが供給されたプログラムコードを実行することにより、上述の実施の形態で説明した機能が実現されるだけでなく、そのプログラムコードがコンピュータにおいて稼働しているOS（オペレーティングシステム）あるいは他のアプリケーションソフト等の共同して上述の実施の形態で示した機能が実現される場合にもかかるプログラムコードは本発明の実施の形態に含まれることは言うまでもない。

【0098】

さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるCPU等が実際の処理の一部または全部を行い、その処理によって上述した実施の形態の機能が実現される場合にも本発明に含まれる。また、上述した実施形態ではメモリ媒体としてカードを例に挙げて説明したが、上記メモリ媒体としてはカード状の媒体のみならず、例えば、スティック状のメモリ媒体であってもよく、形態はかまわない。また、上述した実施形態において、秘密鍵、公開鍵の両方あるいは一方だけを電子署名データとともに格納するようにしてもよい。

【0099】

【発明の効果】

以上説明したように、本発明によれば、メモリ媒体に保存されている署名付き

画像ファイルデータを画像処理システムに転送し出力しようとする場合、上記画像処理システム内で一方向性関数を用いて算出される上記画像ファイルデータのメッセージダイジェスト値と、上記署名を復号する公開鍵を用いて復号化される値とを比較検討することによって、上記画像ファイルデータが改ざんされたかどうか確実に判別することが可能となり、メモリ媒体に格納した画像の信頼性を大幅に向上させることができる。

## 【0100】

また、本発明の他の特徴によれば、ユーザに委ねる選択をプロパティファイルに記述することにより、ユーザはより容易に画像ファイルデータを検証・出力することができる。

## 【0101】

また、本発明のその他の特徴によれば、画像処理システムがネットワークを介してホストコンピュータと接続されていることを利用して、画像処理システム以外のメモリカード(I/F)に接続されたメモリ媒体から、画像ファイルデータを画像処理システムに転送することができ、ユーザはより容易に画像ファイルデータの出力・検証を行うことができる。

## 【0102】

また、本発明のその他の特徴によれば、リーダ部により取り込まれた画像ファイルデータやホストコンピュータにおいて作成された画像ファイルデータをメモリ媒体に保存する際に、一方向性関数を用いて上記画像ファイルデータのメッセージダイジェスト値を算出し、秘密鍵を用いて上記メッセージダイジェスト値を署名し、上記画像ファイルデータとともに上記メモリ媒体に保存するようにしたので、上記画像ファイルデータの改ざんを確実に防止することができ、上記画像ファイルデータの信頼性を向上させることができる。

## 【図面の簡単な説明】

## 【図1】

本発明の実施形態を示し、画像処理システムの概略構成を示すブロック図である。

## 【図2】

本発明の画像出力装置の構成を示す断面図である。

【図 3】

電子署名に関する説明図である。

【図 4】

電子署名に関する説明図である。

【図 5】

電子的データとメッセージダイジェスト値との関連を説明する図である。

【図 6】

メモ리카ードを画像処理システムに接続したシステムの一例を示すブロック図である。

【図 7】

本発明の第 1 の実施形態、第 2 の実施形態、第 3 の実施形態におけるメモ리카ードのメモリマップの一例説明する図である。

【図 8】

第 1 の実施形態に関するプロパティファイルスクリプトの内容の一例を示す説明図である。

【図 9】

第 2 の実施形態に関するプロパティファイルスクリプトの内容の一例を示す説明図である。

【図 1 0】

第 1 の実施形態の処理手順を説明するフローチャートである。

【図 1 1】

第 2 の実施形態の処理手順を説明するフローチャートである。

【図 1 2】

第 3 の実施形態の処理手順を説明するフローチャートである。

【図 1 3】

第 4 の実施形態の処理手順を説明するフローチャートである。

【図 1 4】

第 4 の実施形態の処理手順を説明するフローチャートである。

【図 1 5】

第 1 の実施形態を説明する画像処理システムの操作部の表示例を示す説明図である。

【図 1 6】

第 2 の実施形態を説明する画像処理システムの操作部の表示例を示す説明図である。

【図 1 7】

第 3 の実施形態を説明する画像処理システムの操作部の表示例を示す説明図である。

【図 1 8】

第 4 の実施形態を説明する画像処理システムの操作部の表示例を示す説明図である。

【符号の説明】

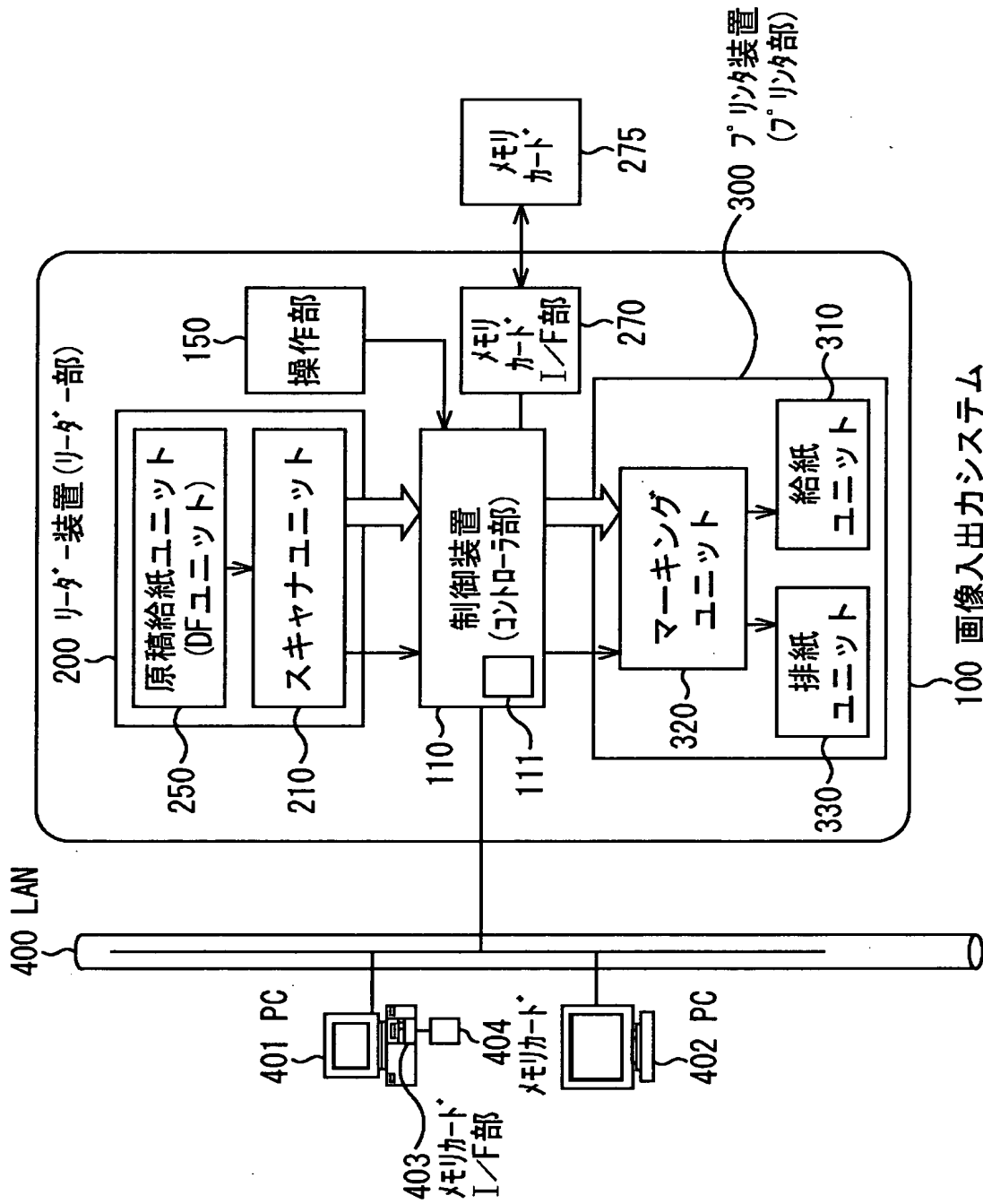
- 1 0 0 画像処理システム
- 1 1 0 制御装置
- 2 0 0 リーダ部（画像入力装置）
- 3 0 0 プリンタ部（画像出力装置）
- 2 1 0 スキャナユニット
- 2 5 0 原稿給紙ユニット
- 3 1 0 給紙ユニット
- 3 2 0 マーキングユニット
- 3 3 0 排紙ユニット
- 2 7 0 メモリカードインターフェース（I/F）部
- 2 7 5 メモリカード
- 4 0 0 ネットワーク
- 4 0 1、4 0 2 ホストコンピュータ
- 4 0 3 メモリカード（I/F）



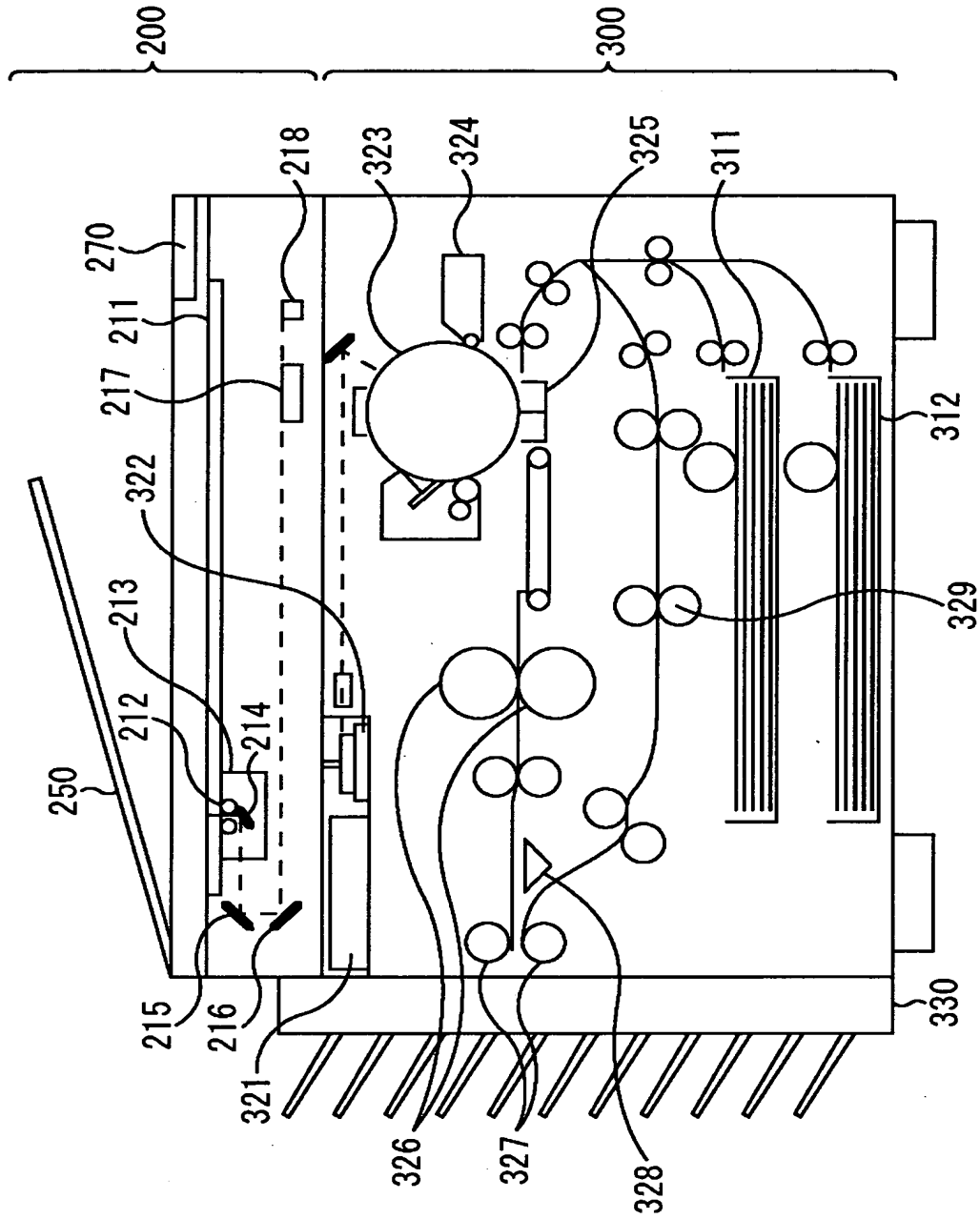
【書類名】

図面

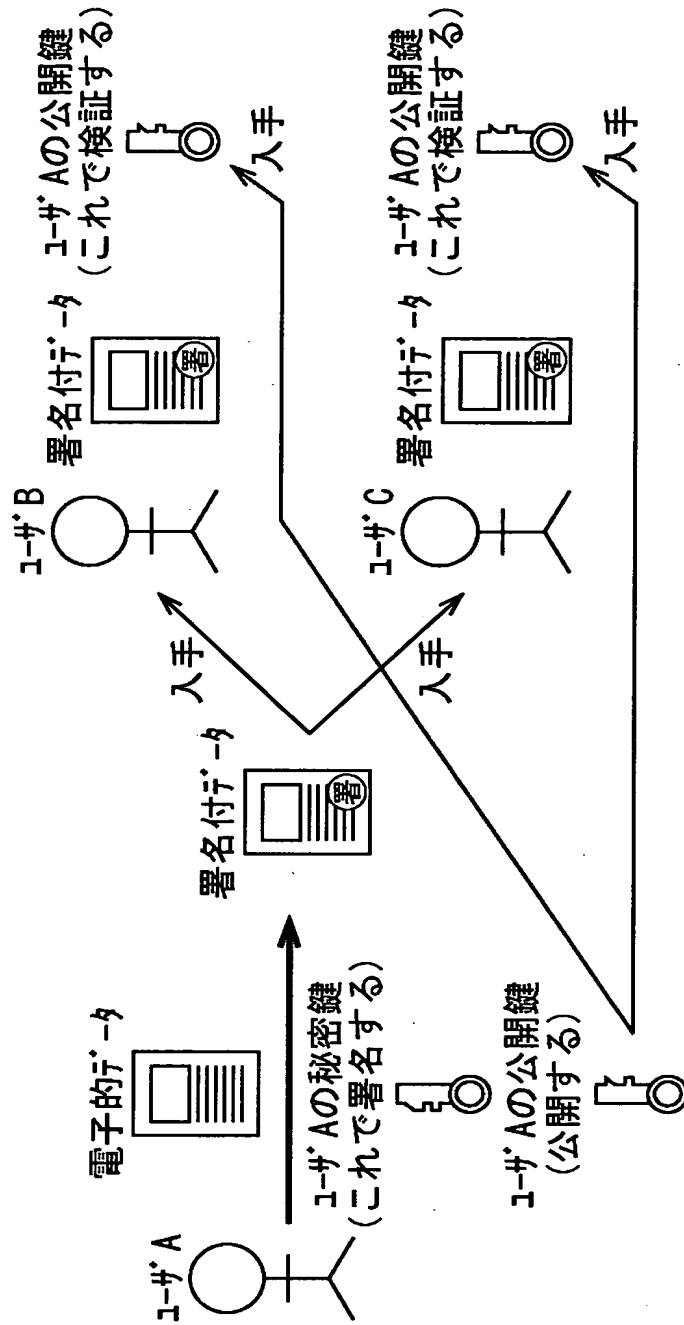
【図 1】



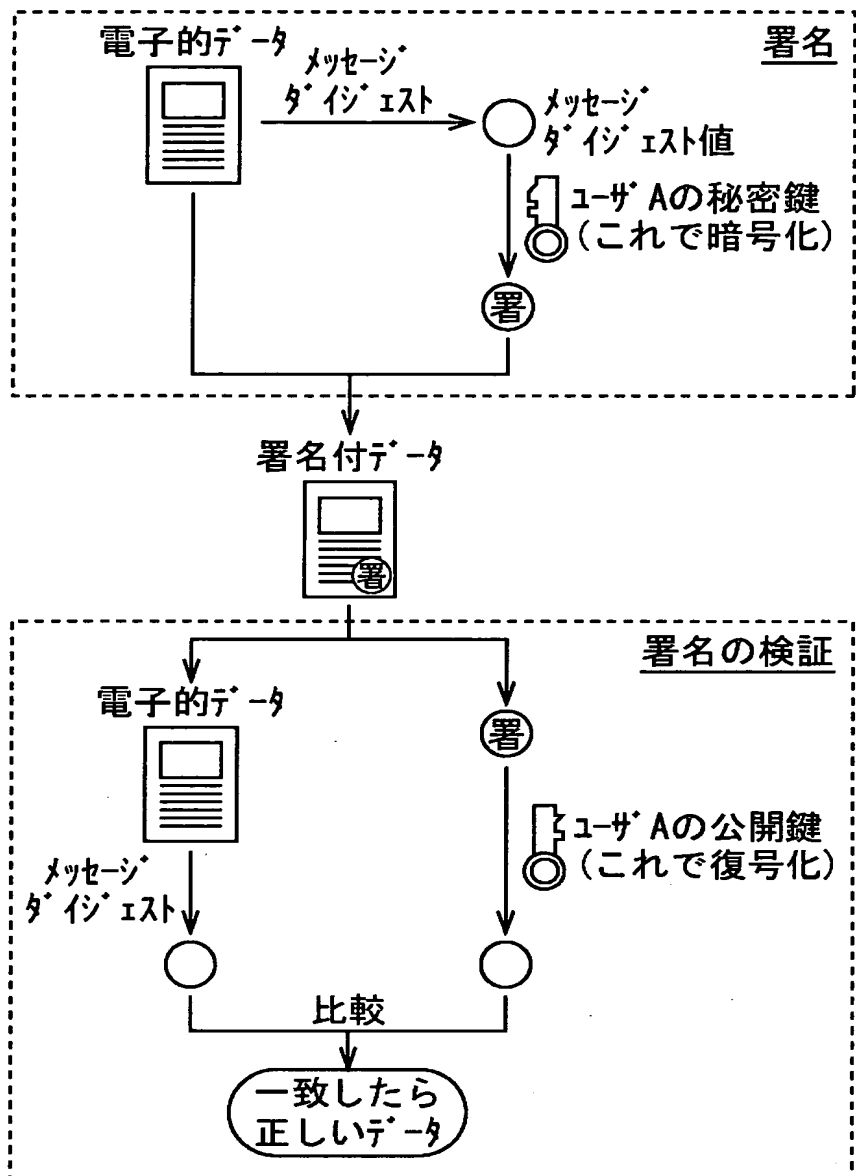
【図 2】



【図 3】



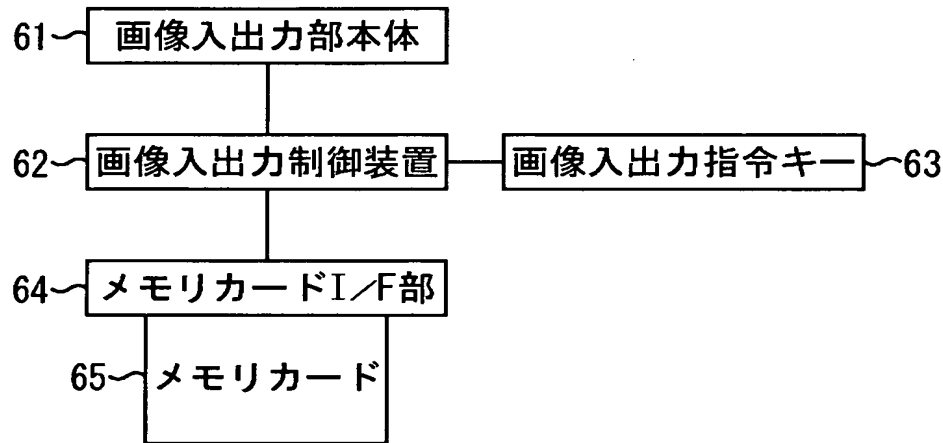
【図 4】



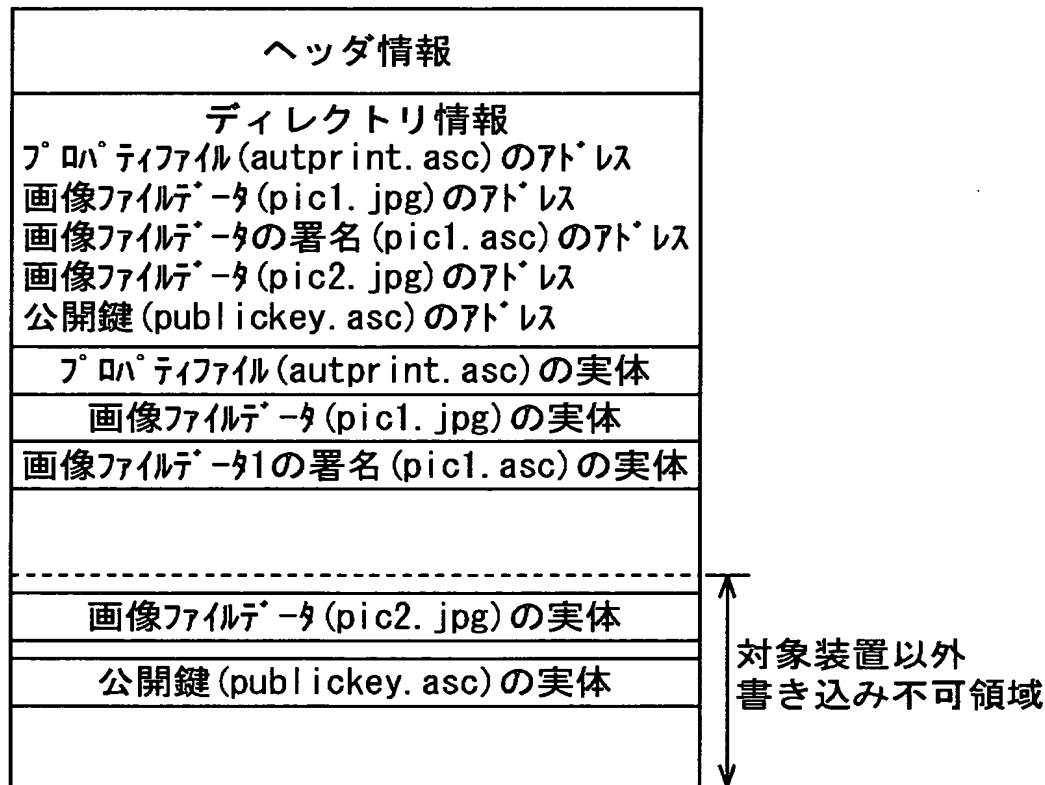
【図 5】



【図 6】



【図 7】



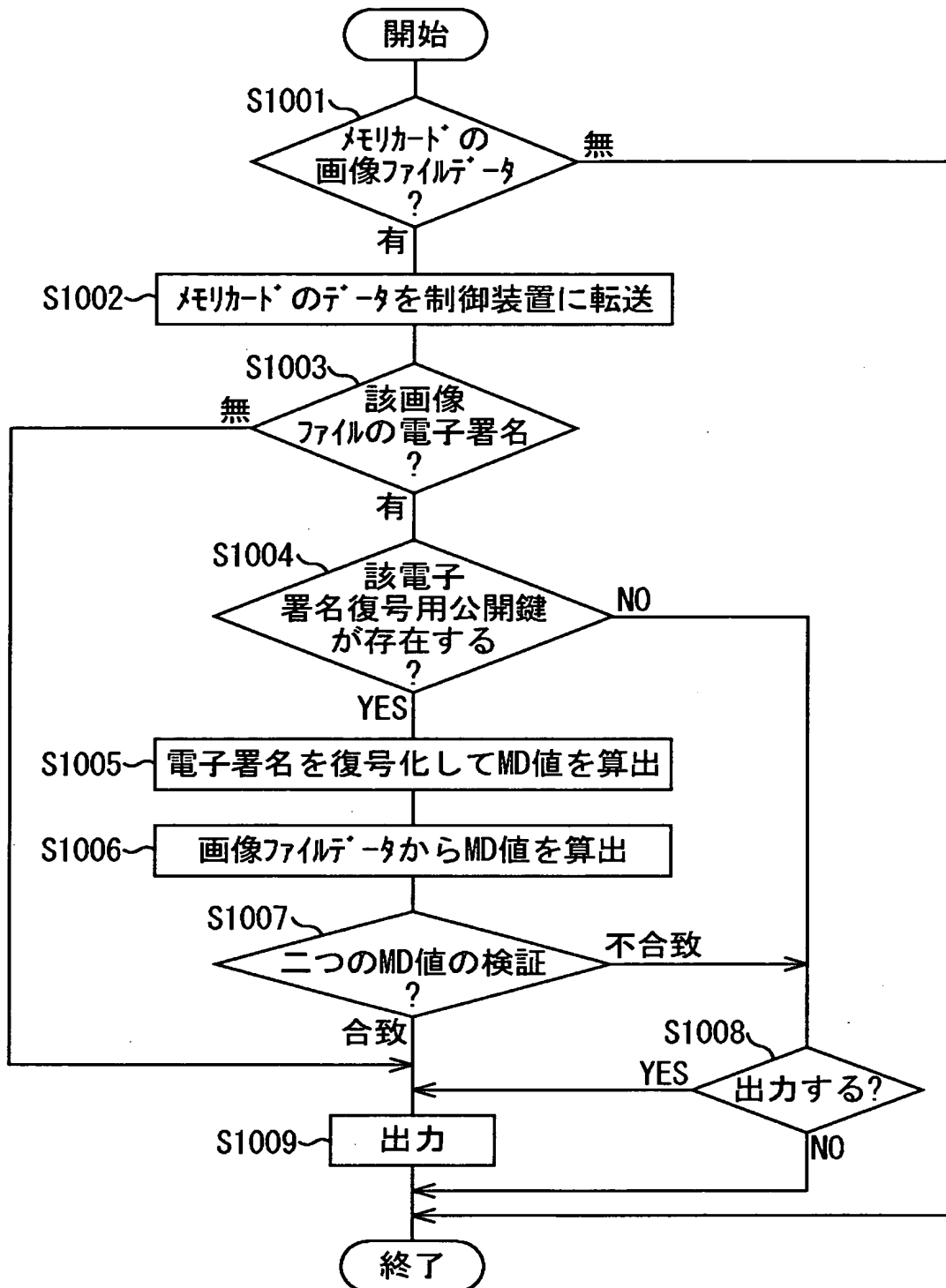
【図 8】

pic1. jpg, A4, SS, 1P

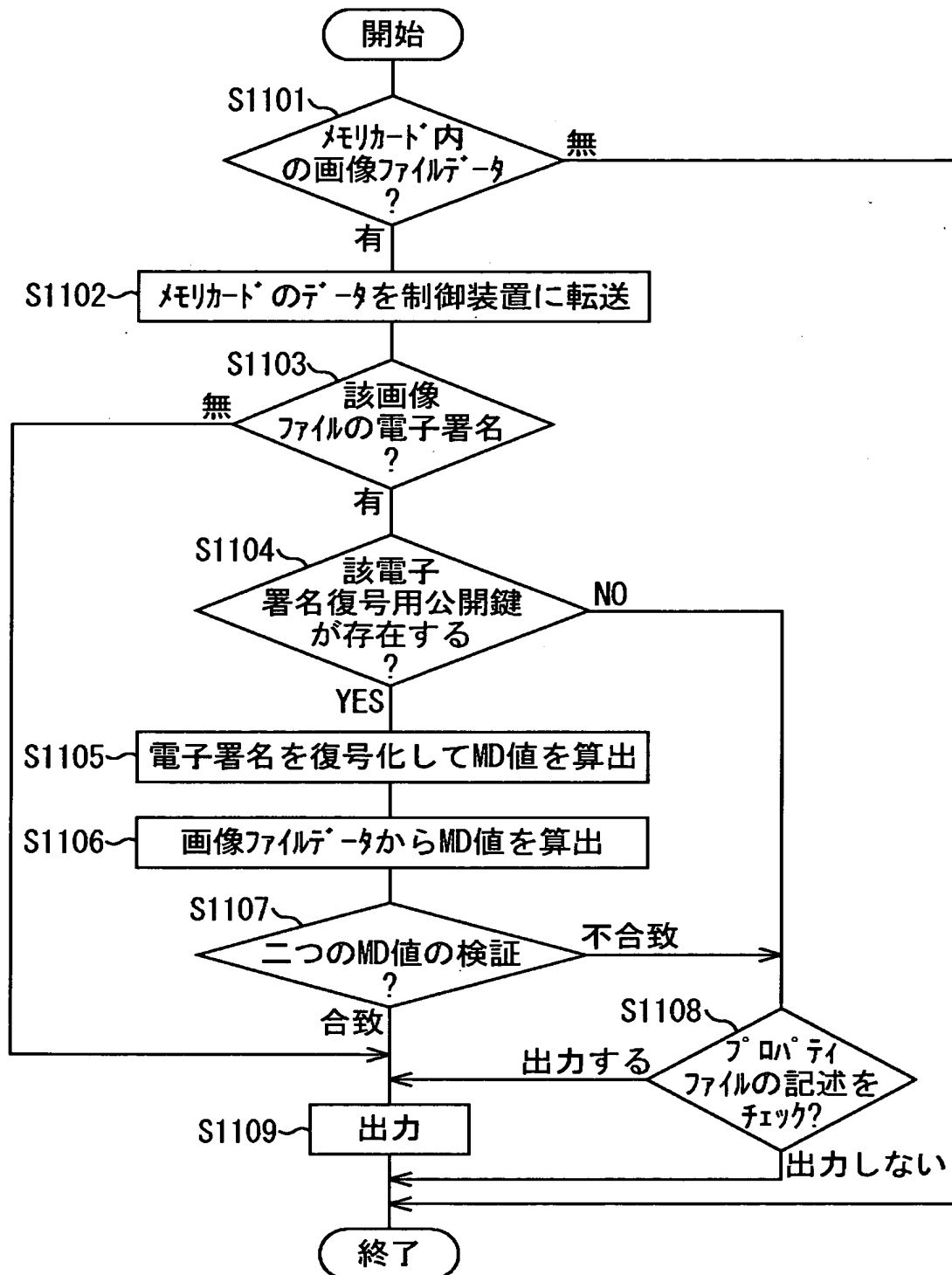
【図 9】

pic1. jpg, A4, SS, 1P, NK1, UMO

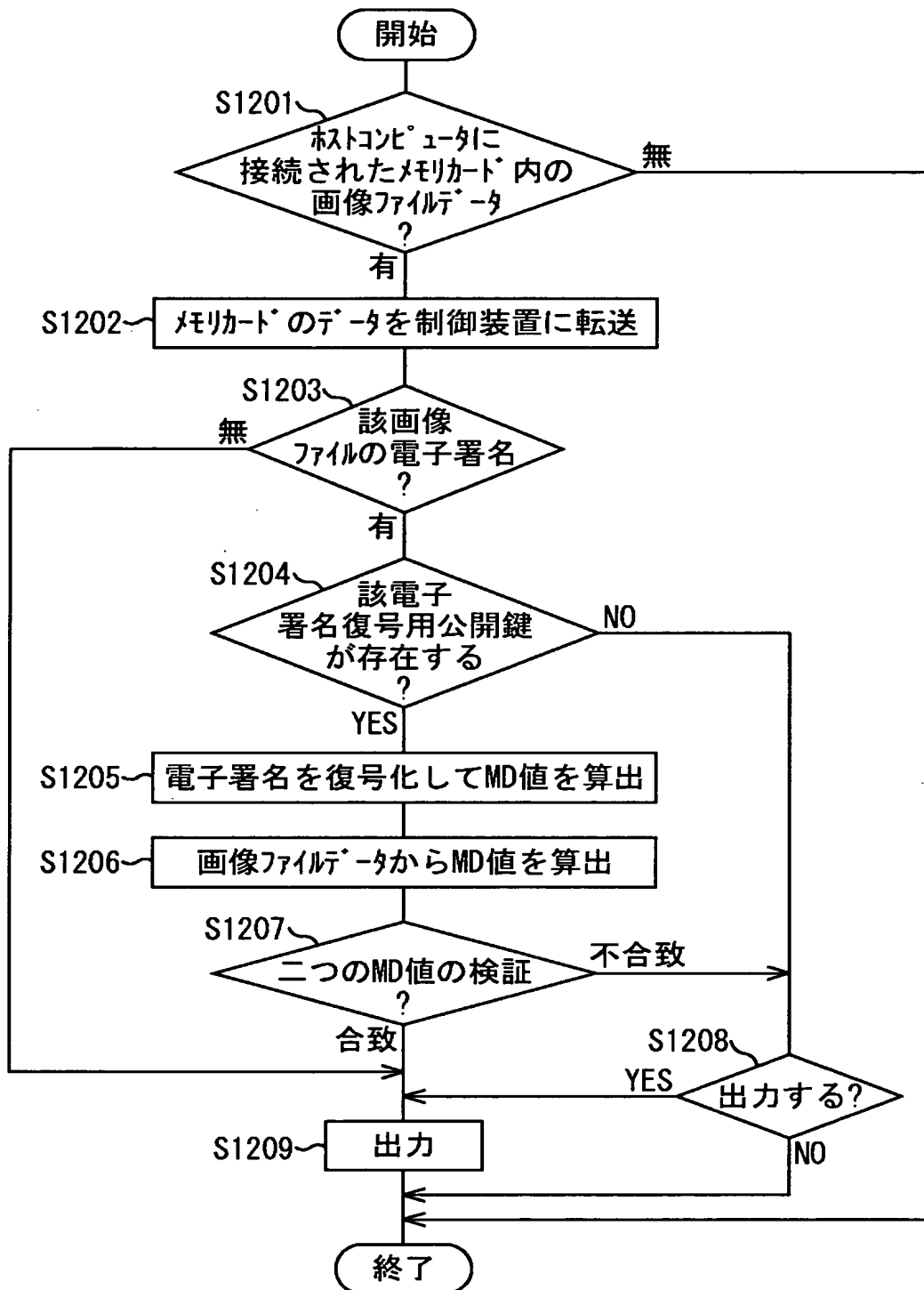
【図 10】



【図 11】

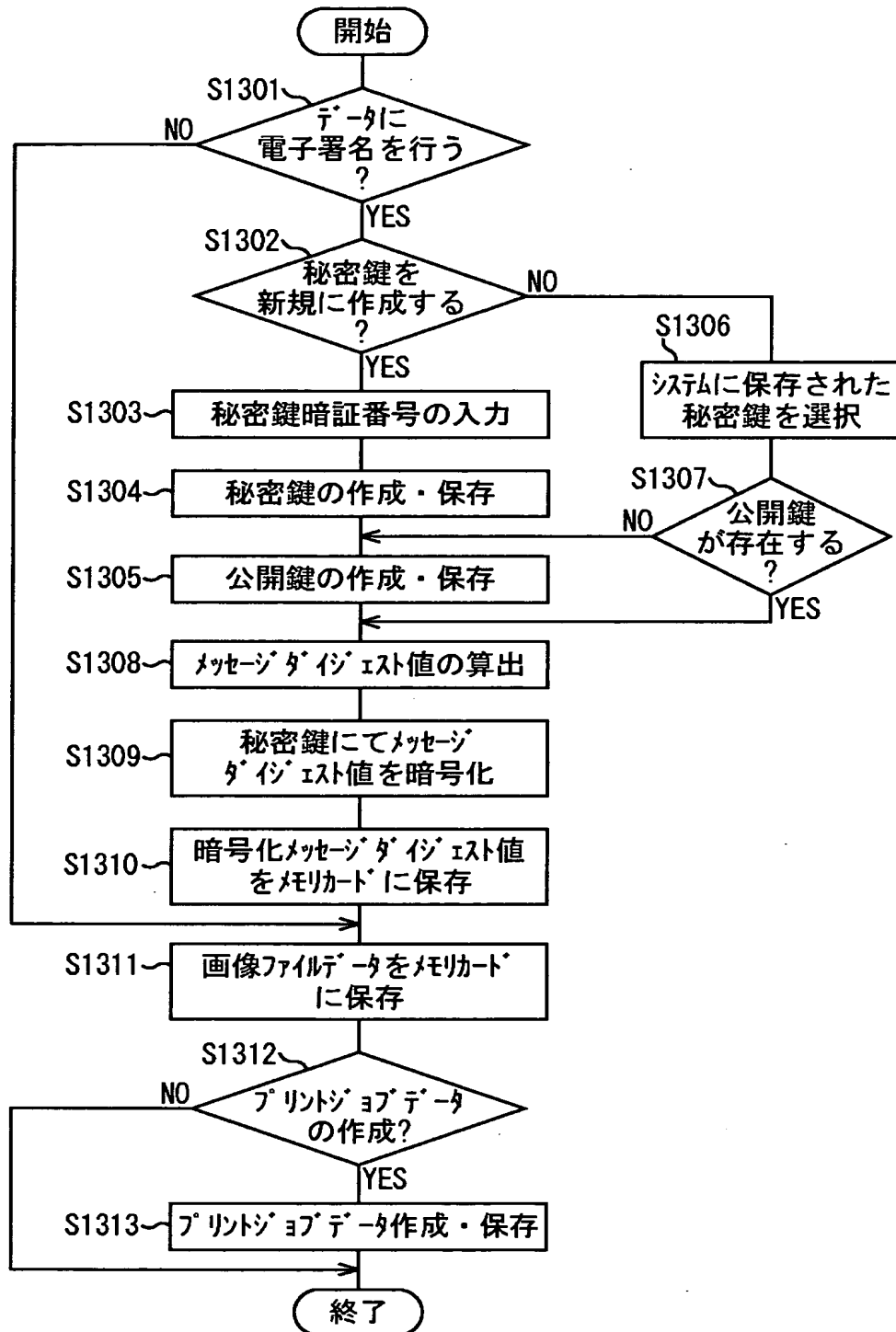


【図 12】

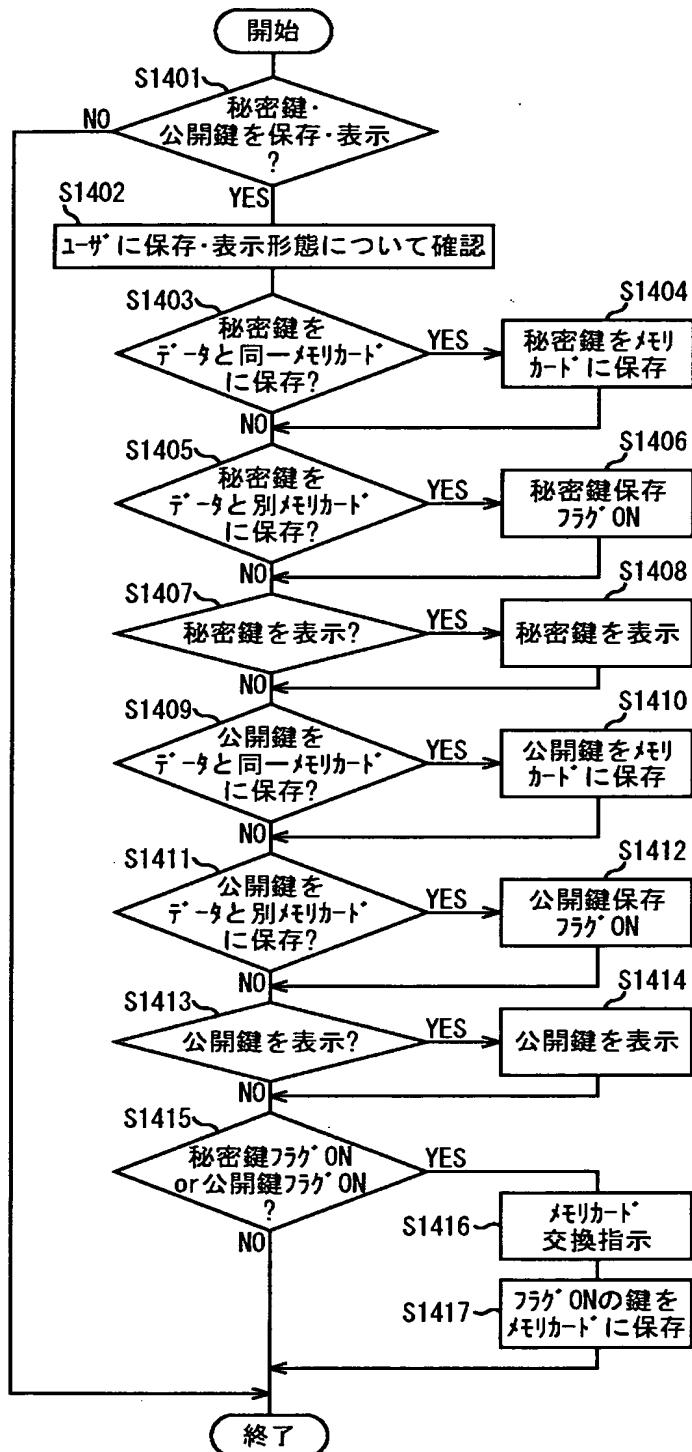




【図 13】



【図 1 4】



【図 1 5】

署名付保存
署名なし保存

【図 1 6】

ファイル名 pic1	ファイル名 A4	両面印刷 片面	出力枚数 1
ファイル名変更	用紙サイズ	出力枚数	
両面	詳細設定	保存	

【図 1 7】

画像、署名、プロパティファイル  
を保存しました。

続いて秘密鍵、公開鍵を保存  
もしくは表示しますか？

YES	NO
-----	----

【図 1 8】

秘密鍵	公開鍵
このメモカードに保存する	このメモカードに保存する
別のメモカードに保存する	別のメモカードに保存する
画面に表示する	画面に表示する

【書類名】 要約書

【要約】

【課題】 メモリカード内の画像ファイルデータの改ざん・偽造を判別できるようにして、画像出力の信頼性を向上させる。

【解決手段】 メモリ媒体に蓄積されている画像ファイルデータに関する電子署名、上記電子署名に用いた秘密鍵、またはその対となる公開鍵を、上記画像ファイルデータ及びプロパティファイルとともに画像制御装置に転送する転送手段と、上記転送手段によって転送された情報に基づいて画像出力を行うように制御する画像出力制御手段とを設け、メモリ媒体に格納されている画像ファイルデータの改ざん・偽造を防止できるようにする。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000001007]

1. 変更年月日 1990年 8月30日  
[変更理由] 新規登録  
住 所 東京都大田区下丸子3丁目30番2号  
氏 名 キヤノン株式会社